



# ARAT BULLETIN



Published by ATRR-PO  
Fort Monmouth, NJ 07703

Volume 3, Issue 1

April 1996



## **RADAR SIGNAL DETECTING SETS: The Lessons Continue!** (See Page 1!)

---

### **What's Inside:**

AN/APR-39A(V)1 (Taking Another Lesson ...)	Page 1	SIPRNET Testing At Joint Exercise INTERNAL LOOK 96	Page 6
SIPRNET Dial-up Access	Page 4	ARAT World Wide Web: An Update	Page 7
WANTED: Joint Uniform	Page 5		

---

# **FAREWELL LETTER**

**Benjamin Franklin once said “... in this world nothing is certain but death and taxes.” “Change” should be added to that axiom. In my three plus years as the Project Manager for the Army (Target Sensing Systems) Rapid Reprogramming Project Office (ATRR-PO), change has been a constant presence. The task of implementing an infrastructure from scratch to support rapid reprogramming of Army Target Sensing Systems (ATSS) has been a daunting one.**

**The diversity of reprogramming-related activities taking place today throughout the Army is indicative of reprogrammings’ growing importance. The ATRR-PO recognized the need to educate the Army community in order to create and maintain an awareness of reprogramming activities. This is being achieved through several means to include publication of the ARAT BULLETIN, and sponsorship of training classes for areas such as EO/IR and EWIRDB.**

**Technical approaches for field reprogramming of ATSS have been identified, studied, and evaluated with our focus primarily in the Army Aviation community. One key method uses the Memory Loader Verifier (MLV), currently undergoing field testing on a limited basis in troop units, to reprogram ATSS. Recent demonstrations have proven the technical viability of the ARAT WAN in providing reprogramming data from CONUS to field units during Exercise BRIGHT STAR 95.**

**The time required to reprogram ATSS has been reduced from months down to days in the past several years. We, the Army reprogramming community, have made tremendous progress, but my successor, Mr. Joseph Ingrao, still faces many challenges in order to achieve the Army’s goal of providing a rapid reprogramming capability to the field in a matter of hours. As I depart, I want to extend my thanks to everyone who has supported the ARAT “cause” and who has shared in the frustrations and accomplishments. I leave with the knowledge that the project is in good hands both at SED and ARAT-TA, Eglin AFB. I challenge you to continue your present course under the leadership of the new ATRR Project Office Chief, Mr. Joseph Ingrao.**

**SOK KIM**

# THE ROLE OF THE AN/APR-39A(V)1 RADAR SIGNAL DETECTING SET

## ...Taking Another Lesson From Desert Shield/Desert Storm (DS/DS)

*It was early in the combat operations phase. We were part of the Eagle Deep strike package, a Brigade-size Task Force. Our mission was to provide a screen along the division's flank to help provide a shoulder for follow-on deep strikes. The S2 gave a good threat brief for the mission but the mobility of anti-aircraft artillery (AAA) and surface-to-air missiles (SAMs) prevented an accurate grid location, even though we knew they were out there. Our pilots had the best training and we had high confidence in our ability and that of our Apache and OH58D team. About 15 minutes across the line-of-departure, our APR39A(V)1 Radar Signal Detecting Set (RSDS) alerted us to the deadly AAA guns that lay in ambush for us. The new Mission Data Set (MDS) installed by our Electronic Warfare Officer (EWO) for this geographical region told us the AAA threats were there. Our RSDS showed the AAA radars that were tracking our flight, waiting for us to get within gun range--long before we could get visibility on them. The enemy had done their intelligence preparation of the battlefield (IPB) well. The RSDS visual and aural warnings of "GUNS TRACKING" cued us when the AAA radars illuminated our Apaches. We adjusted our flight route just in time. Within seconds of our turn, we could see the 23mm illumination rounds coming in our direction--landing short of their targets. We continued our mission and provided the combat information to the scouts. In short order, the scouts sent targets to our support artillery, which raised havoc with the threatening AAA guns and their radars.*

In this scenario the RSDS provided pilots with the timely, Electronic Warfare (EW) picture of the battlefield situation. Situational awareness was possible because the aircraft were equipped with the right software packages for the RSDS processor and the updated hardware, just as required in the real-world.

The AN/APR-39A(V)1 RSDS is a passive Electronic Intelligence (ELINT) system used on Army avionics platforms. There are two components to the RSDS software. First is the

Operational Flight Program (OFP) used to synchronize the functions among the processor, antennas, and the MDS. The second is the MDS, which contains the radar threats and their electronic parameters that are unique to a specific geographical region. The updated spiral antennas provide extended frequency range. The Army Materiel Command (AMC) has a developmental and fielding role here. The AMC will install the newly tested and approved OFP version number 23.9. Likewise, the aviation unit itself has a big role here.

The unit's Electronic Warfare Officer (EWO) by virtue of his operations (S/G3) position and hopefully, EW training, is the staffer with the specific responsibility for the unit's electronic combat capability. As planning time-lines get shorter, the EWO must be included and deliver as a creditable member of the commander's planning staff. The goal of the unit EWO is to reduce unit risks to pilots and aircraft and increase mission success. The EWO responsibility will likely continue to grow as the Army increases reliance on electronic warfare and battlefield situational awareness in the era of Information Warfare.

The pilot's electronic combat (EC) situational awareness is aided with the relatively new RSDS. Depending on the aircrew's mission and location on the battlefield, this system can support the pilot in all three components of EC--Electronic Attack (EA), Electronic

**(Continued Next Page)**

## AN/APR-39A(V)1 (Continued)

Protection (EP), and Electronic Support (ES). To be most effective, the unit EWO must keep the aircraft's processor current with the MDS written for his mission area. Once in theater, the EW information on the Bulletin Board System (BBS) continues to be updated and available to the EWO 24 hours a day.

Actual time conducting reprogramming of the typical aviation unit is minimal. Once the EWO has registered his STU-III telephone with the BBS, it should only take a nominal amount of time to down-load the appropriate MDS, radar threat notes, and pilot kneeboard sheets. Once the information is downloaded into the EWOs PC or laptop, it can be quickly connected and reprogramming of each aircraft's RSDS processor can be completed.

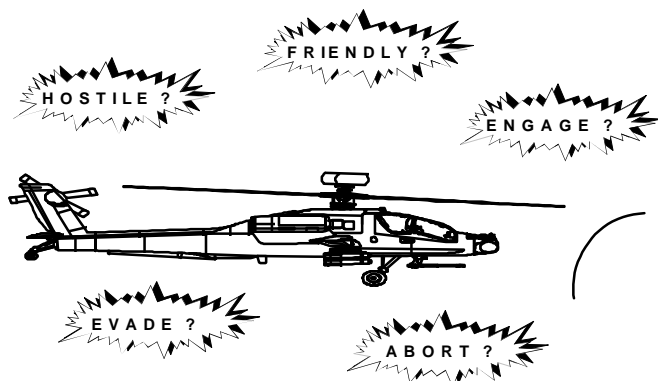
All major geographical world regions have a specific MDS written and resident within the BBS menu files. The Army Reprogramming Analysis Team-Threat Analysis (ARAT-TA) initiates the MDS process which begins with detailed electronic warfare analysis of the geographical region. The team goes through the analysis focusing on the threats as seen from the helicopter's mission profile. There are two primary reasons that might require a new MDS. First is a new threat system may have moved into the mission area of interest. The other reason might include a deliberate attempt to operate threat radars in a new part of the electro-magnetic spectrum in order to alter a radar's electronic "finger-print." The threat might employ any combination of these methods as a part of their Wartime

Reserve Mode (WARM) operations. All these actions are an attempt to counter our capability to map the various threat radars used in target acquisition, tracking, and guidance.

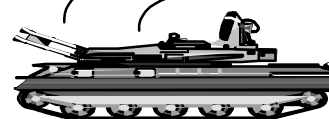
The unit EWO can have a dial-up capability to the BBS from anywhere in the world. Once connected, the EWO can get a software download of the MDS for the desired mission area from the multiservice Electronic Combat Bulletin Board Service (BBS). The Army Reprogramming team along with the Air Force Reprogramming Flight maintain the secure BBS. The BBS communications link can be provided to tactical locations via commercial phone line if adequately planned for through coordination with the unit's signal officer. An alternate communications path will soon be demonstrated as well. The Secure Internet Protocol Router Network (SIPRNET) to Mobile Subscriber Equipment (MSE) will also provide the tactically deployed EWO with access to the BBS. The tactical

(Continued Next Page)

### Battlefield impact with current software Mission Data Set...



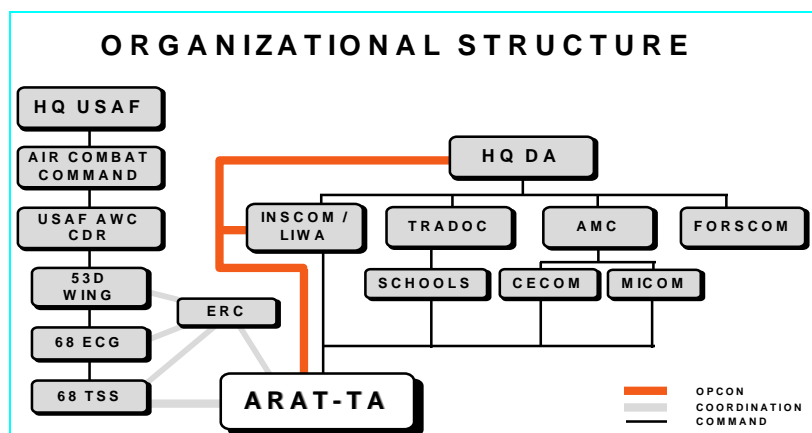
- Timely and accurate identification of threat
- Use of correct electronic attack, protection, and identification (EA/EP/ES) techniques



**Results:** → Less Risks to Aircrew & Aircraft  
→ Higher MSN Success

## AN/APR-39A(V)1 (Continued)

connectivity is available with organic systems. The Reprogramming team in cooperation with the Air Force and Navy has recently demonstrated the BBS connectivity to the Army's RSDS while aboard the Navy carrier, USS Kennedy, 150 miles off the east coast of Florida. You might recall mission and staging considerations placed the 10th Mountain Division's Aviation Brigade aboard a Navy carrier while awaiting deployment to Haiti. Using available technology, the unit EWO can have access to sensitive electronic warfare information regardless of the time or place; during any phase of combat operations.



To ensure connectivity with the BBS and MDS files, the unit EWO should register the unit's STU-III telephone with the BBS system managers. Upon completing this, the unit EWO simply dials the BBS and receives immediate access. The telephone's key registration number provides BBS access and also provides information security. The PC or laptop will need communication software application that is provided to the unit. With these commonly available resources the EWO has the capability to gain access to the BBS and download the desired MDS for his contingency area. The Army Reprogramming team can get the communications software and PC-to-RSDS processor cable (RS232 and J3 plug) for the EWO. The unit must provide the STU-III and a PC or Laptop.

Unit EWOs receive training on the Army Reprogramming process at Fort Rucker during a relatively new 2 week EW course. Intelligence analysts and engineers at the Army Reprogramming office at Eglin also routinely provide expertise on the technical issues related to BBS access procedures.

Many Army aviation battalions have aggressively moved to leverage the technology provided by the Army Reprogramming

infrastructure. The Reprogramming Analysis Team works with the dedicated software Reprogramming engineers at CECOM. Together the teams also are aggressive in their pursuit to provide a "Direct Support" attitude towards Reprogramming and Army Aviation. Special operations aviation units are using the Army's Reprogramming capability to support their unique mission requirements. Prior to their January '96 NTC rotation, the 1-227th Attack Battalion, 1st Cavalry Division welcomed AMC and the Army Reprogramming team at Fort Hood to install the latest OFP hardware and software. The 1-227 Attack Battalion used the rapid reprogramming capability at the NTC by demonstrating the BBS-to-aircraft process downloading the MDS written for the NTC's ASET IV radar threat simulator. The FORSCOM G3 aviation office and NTC's Eagle Team and Simulations Branch are credited for their effort to improve EW situational awareness in Army aviation cockpits.

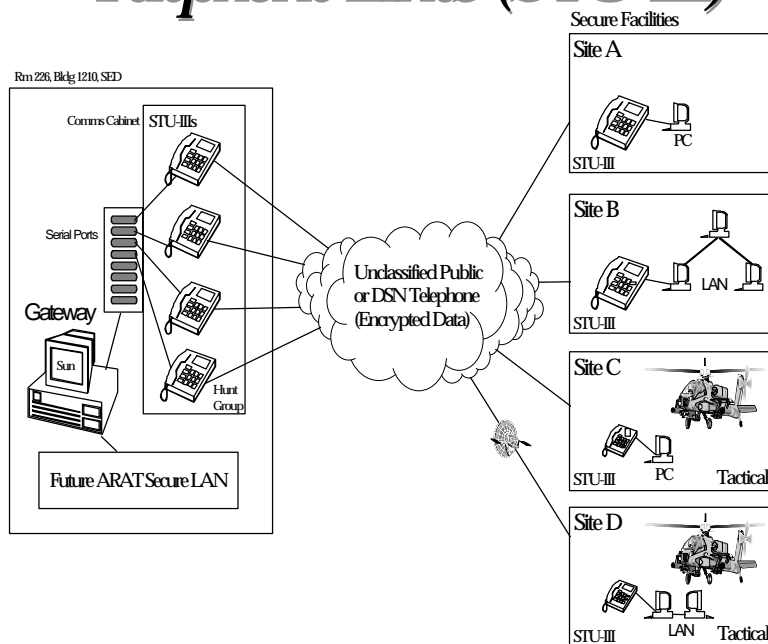
Similar scenarios like the one at the beginning of this article occurred many times during the Middle East war. The RSDS with the right MDS and OFP can play a critically important role for aircrew and aircraft survivability and mission success. The intent of these tools is not to relieve the unit of its requirements for Intelligence Preparation of the Battlefield (IPB) and intelligence briefing. With good pre-mission planning and these electronic combat tools, the aviators can take a lesson learned from the DS/DS war and enhance their battlefield EW situational awareness. POC is LTC Don Adkins, DSN 872-8899/8919; Comm: (904) 882-8899/8919. His Email address is: AdkinsD@WG53.Eglin.af.mil.

# ARAT Site Connectivity: Dial-up Access To SIPRNET

## Part V in a series

This is the fifth article in a continuing series on the ARAT Wide Area Network (WAN). Part I (1/95) described ATRR-PO's rationale for establishing a WAN. Part II (4/95) delved further into various WAN connectivity options. Part III (10/95) highlighted the establishment of Secure Internet Protocol Router Network (SIPRNET) connectivity. Part IV (1/96) detailed the successful rapid transmission of reprogramming data over SIPRNET to an overseas deployed site recently during a major exercise. Part V discusses how ARAT community users can gain access to SIPRNET through STU-III dial-up methods.

## *Implementation: Telephone Lines (STU-III)*



Within the past several months, the ATRR-PO has implemented a dial-up capability to SIPRNET in the Rapid Reprogramming Communications Infrastructure Laboratory (R2CIL). There is currently one line operational with additional lines planned for activation in the near future.

As previously mentioned, the Project Office is still considering specific PC software applications to be provided to ARAT community personnel on floppy diskette if needed to achieve the desired connectivity. Users who already have the appropriate software available should proceed and call the Project Office if specific technical assistance is needed or if problems arise that cannot be handled by the local computer support staff. ARAT community users who desire dial-up access into SIPRNET must complete an account request form available from the Project Office.

There is now also another method of dial-up access into SIPRNET. DISA recently announced the establishment of a 1-800# service. In order to use this capability, users need to first acquire an account with Email capability on an existing SIPRNET host (like the ATRR-PO's in the R2CIL). Users must then fill out a separate set of forms which are sent to the Army POC at Fort Huachuca, Ms. Linda Jones, DSN: 879-6840 or Comm: (520) 538-6840. As this is a new DISA initiative, the Project Office is gathering additional information which it hopes to provide to the ARAT community at the March IPR.

(Continued Next Page)

---

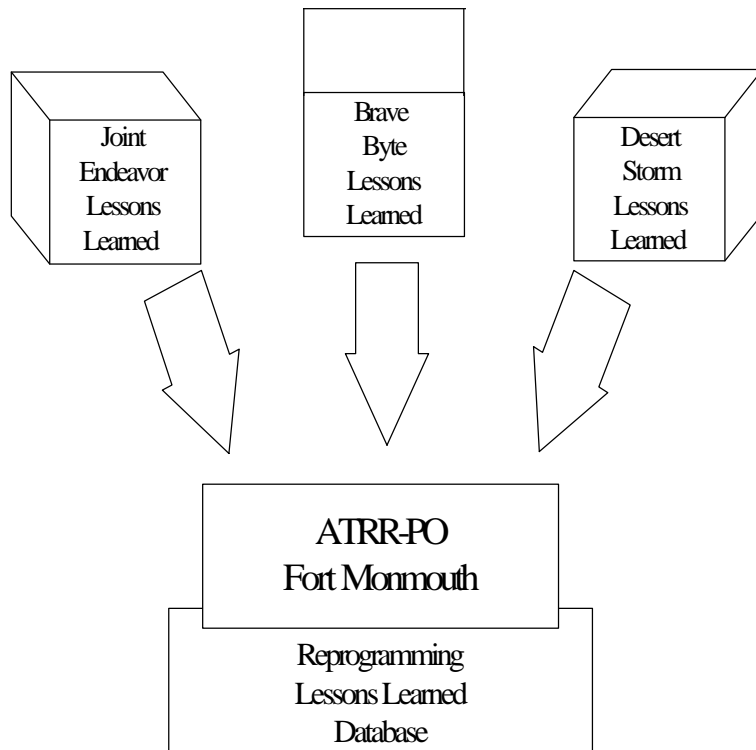
## ARAT Site Connectivity (Continued)

Future articles will provide updates concerning progress and changes relating to the WAN. POCs are Mr. Ken Kragh, DSN: 992-6003/Comm: (908) 532-6003 or Ms. Jacki Yamello, DSN: 987-6000/Comm: (908) 427-6000.

---

# WANTED!!

## Army Reprogramming Lessons Learned



The ATRR-PO is collecting Army Reprogramming Lessons Learned and will add these lessons to the Training and Readiness Section of the ARAT HomePage on SIPRNET. We need your help in capturing reprogramming lessons learned during daily, exercise,

and contingency operations. Share your experience(s) and solution(s) with the rest of the Army Reprogramming community. You can submit your Lessons Learned in one of three ways:

1. Use the Joint Universal Lessons Learned System (JULLS), Version 5.1 or earlier. Place the lesson(s) on a 3.5" disk and mail to the ATRR-PO at the address below.
2. Use the electronic form available in the Training and Readiness section of the ARAT HomePage on SIPRNET.
3. Use the form enclosed in this issue and mail to the ATRR-PO at the address below.

**ATRR-PO**  
**c/o SED Security**  
**Office**  
**CECOM RDEC SED**  
**Bldg. 1210**  
**Fort Monmouth, NJ**  
**07703**

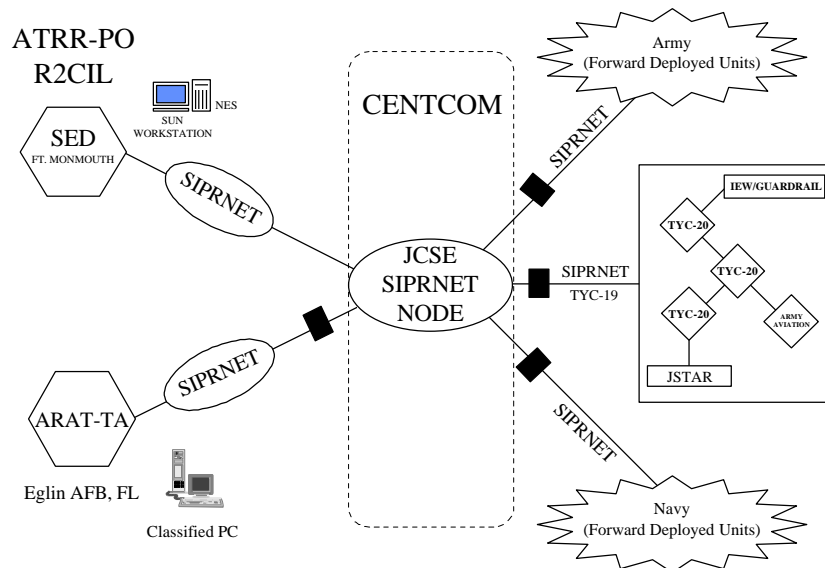
---

To receive this publication,  
submit the following:

- \* Organization
- \* POC
- \* Address
- \* Phone/Fax #

Fax to: (908) 532-5238 (U) or  
DSN: 992-5238 (U)

Or send via Email to:  
[arat@iew.sed.monmouth.army.mil](mailto:arat@iew.sed.monmouth.army.mil)



## Army SIPRNET Tested During Joint Exercise

The Army (Target Sensing Systems) Rapid Reprogramming Project Office (ATTR-PO) is charged with developing an infrastructure to support rapid reprogramming of Army Target Sensing Systems (ATSS). As part of this effort, the ATTR-PO periodically participates in Army and Joint Service exercises to test and evaluate various components of this infrastructure. Thus, the ATTR-PO recently participated in a U.S. Central Command (CENTCOM) Joint Service Exercise.

ATTR-PO representatives worked with the CENTCOM Joint Staff (J2/3/6) and CENTCOM Joint Communications Support Elements (JCSE) to provide electronic warfare (EW)/threat analysis support and rapid software updates in support of CENTCOM's mission essential tasks and responsibilities from the theater level on down to the operational level. Several different key functions of the ATTR-PO staff were successfully exercised during the course of this exercise. In addition, validation was performed of ATTR/Joint EW Officer (JEW) tasks supporting the CENTCOM mission.

The ATTR-PO simulated threat detection to Joint Aviation Radar Signal Detecting Sets (RSDS) at a deployed CENTCOM Joint Command & Control Operations Center (JCC-OC) location. Data was transmitted via Secure Internet Protocol Routed Network

(SIPRNET) to the Army Reprogramming Analysis Team Threat Analysis (ARAT-TA) cell for validation. Data was then forwarded to the ATTR-PO Rapid Reprogramming Computer Information Laboratory (R2CIL) at Fort Monmouth for reprogramming and transmission back to the JEW cell in the field. The accompanying diagram depicts the general flow of reprogramming information out to Army forward-deployed units over the SIPRNET.

The ATTR-PO will be conducting additional tests using the SIPRNET as it continues to set up a reprogramming infrastructure for the Army. Any one who desires additional information about these efforts should contact the ATTR-PO at Fort Monmouth. POC is Mr. Ken Kragh, DSN: 992-6003/Comm: (908) 532-6003.



---

# **The ARAT World Wide Web (WWW)**

## **Part II In A Series**

The ARAT WWW HomePage on SIPRNET continues to grow. Since its' first mention in these pages some six months ago, considerable progress has been achieved. Through the guidance of the ATRR-PO and the technical expertise of the ARAT, a content hierarchy has been developed and established. This hierarchy defines products and services to be provided via the new WWW technology which are designed to provide enhancements to the reprogramming process.

The ARAT WWW now holds a wealth of information related to the project office which includes the mission statement, frequently asked questions, and a reprogramming terminology repository. A clickable United States map is available which provides all the Points of Contact for the various ARAT cells. This information is being described as static "products." The ARAT has defined products to be those static pieces of information which describe the Project Office and its' workings (i.e., information that seldom changes). More information is being added all the time as legacy documents are converted into HTML. Such additional work is being done with this very document, the ARAT BULLETIN. All back issues, as well as the current issue, will be made available on-line in the near future.

The most exciting work done on the ARAT WWW over the past six months can be referred to as the "services." Services such as Email, chat, BBS link, file upload/download, and audio/video training provide for the improvement of reprogramming. These services are aimed at enhancing collaboration and thereby the reprogramming mission.

Services currently being offered include or will include a training and readiness section that links to ARAT briefing repositories to be used as training modules, a direct connection to the ARAT BBS for the downloading of pertinent threat information, a link to SIPRNET-based Email for ARAT sites to exchange communications, and a link to select JULLS documents related to reprogramming exercises that is searchable through easy-to-fill-out on-line forms. These services continue to expand and are made available as they mature. Additional services which will provide audio and video content to enhance training, a file upload/download area for software distribution, and a chat and news system are currently under development. All of this information is easily searchable through a self-indexing form.

One of the most recent developments, and probably the most useful for our reprogramming efforts, is the creation of an on-line forms implementation of threat messages. Through the use of a fill-out form, threat messages can be entered, tracked, and reviewed in a unified format across services. This will greatly enhance the distribution and incorporation of current information into the reprogramming process.

The ARAT is looking at the Netscape 2.0 browser client with plug-in extendibility to provide even further enhancements in the way of audio, video, and PDF documents distribution. The Project Office will evaluate these tools based on enhancements to reprogramming and any plug-ins will be made available to the ARAT community for download from the WWW HomePage as they are accepted and implemented.

Access to the ARAT WWW HomePage requires a SIPRNET-connected PC or UNIX workstation and a WWW browser. Netscape is the preferred browser for the ARAT pages but Mosaic will work just as well. Due to the advance HTML that is used here, it is recommended that the latest version of any browser is used.

If you are lacking a SIPRNET connection, please see the WAN article in this issue which describes several methods available for acquiring SIPRNET connectivity. The ARAT is providing this service locally for easy access to the ARAT WWW HomePage, but other, higher speed and more permanent options are also available.

**(Continued Next Page)**

## ARAT World Wide Web (Continued)

In addition, the software required can also be provided to you on diskette if necessary.

In the meantime, if you have the means, please feel free to see what is available now at <http://206.37.16.100> and click on the usage graph to see just how effective this medium is for reaching the ARAT community as a whole. POCs are Mr. Ken Kragh (DSN: 992-6003/Comm: 908-532-6003) or Ms. Jacki Yamello (DSN: 987-6000/Comm: 908-427-6000).

The “ARAT BULLETIN” will be published quarterly and is intended to provide the ARAT Community with current information. You are invited to submit input for improving this publication, or present articles which will be of interest to our readers. You may fax correspondence to the Editor at (908) 532-5238/DSN: 992-5238. Include your name, telephone number, and source(s) of information.

